Abstract

Methods and systems for detection and/or prevention of network attacks can include the use of multiple and/or time-dependent addresses coupled with filtering by the directory or naming service. The directory service can respond to requests for the address of a resource by returning an address that can be relocated over time by coordinating the directory service entry with the host and network address configuration data and/or by returning an address specific to the requestor. Thus, the directory service can track and build profiles of matches between requestors and accesses. The methods and systems can use the time dependent addresses and profiles to distinguish legitimate accesses from unauthorized or malicious ones. Requests for non-valid addresses can be misdirected to "empty" addresses or to detection devices.